UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/782,678	02/19/2004	Daniel J. Zigmond	MS1-1838US	5266

22801 7590 03/09/2006

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
AGWUMEZIE, CHARLES C	
ART UNIT	**PAPER NUMBER**
3621	

DATE MAILED: 03/09/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/782,678	ZIGMOND ET AL.	
	Examiner	Art Unit	
	Charlie C. Agwumezie	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *02/19/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-42, are rejected under 35 U.S.C. 102(e) as being anticipated by Mohammed et al U.S. patent Application Publication No. 2003/0028488 A1.

1. As per **claim 1 and 10**, Mohammed et al discloses a method comprising:

forming a request by a client to access encrypted content, wherein:

the request includes a persistent license for communication to a licensing server (see figs. 5 and 13; 0017; 0155; 0156); and

the persistent license includes a key that is encrypted such that the key is not accessible by the client (0016; 0017); and

receiving a license in response to the request, wherein the received license includes the key that is:

accessible by the client (0016); and

for accessing the encrypted content (0016; 0017; 0018).

2. As per **claim 2**, Mohammed et al further discloses a method, further comprising:

forming an initial request for:

communication to the licensing server (fig. 1 and 5; 0135; 0137); and

storing encrypted content by the client (0116);

receiving the persistent license at the client in response to the initial request (fig. 1, 5, 6, 7 and 13; 0135); and

storing the encrypted content and the persistent license by the client (see figs. 1, 5 and 14; 0185).

3. As per **claim 3**, Mohammed et al further discloses a method, further comprising:

forming an initial request by another client for:

communication to the licensing server (fig. 1 and 5; 0135; 0137); and

storing encrypted content by the other client (0116);

receiving the persistent license at the other client in response to the initial request (fig. 1, 5, 6, 7 and 13; 0135);

storing the encrypted content and the persistent license by the other client (see figs. 1, 5 and 14; 0185; 0130); and

obtaining the persistent license by the client from the other client (fig. 6).

4. As per **claim 4**, Mohammed et al further discloses a method, wherein the

received license is a boundary license and the key is a boundary key, and further comprising:

decrypting a session license utilizing a client key to obtain a session key (see figs. 6 and 8; 0013; 0050; 0055; 0118; 0121);

decrypting the boundary license utilizing the session key to obtain the boundary key (see figs. 6 and 8; 0013; 0050; 0055; 0118; 0121);

decrypting a content license utilizing the boundary key to obtain a content key (0050; 0055; 0118; 0121);

and decrypting the encrypted content utilizing the content key (figs. 5 and 10).

5. As per **claim 5**, Mohammed et al further discloses a method, wherein:

the session license includes access rules for the client for a session initiated between the client and the licensing server (0002; 0009);

the boundary license includes access rules for the client for the encrypted content that is within a rights boundary in the encrypted content (0050); and

the content license includes access rules for the client for the encrypted content (0050).

6. As per **claim 6**, Mohammed et al further discloses a method, wherein:

the persistent license was encrypted using an asymmetric encryption algorithm (0079); and

the encrypted content, the boundary license, and the content license were encrypted using respective symmetric encryption algorithms (0050).

7. As per **claim 7**, Mohammed et al further discloses a method, further comprising:

decrypting a session license utilizing a client key to obtain a session key, wherein the session license includes access rules for a session initiated between the client and the licensing server (fig. 13; 0002; 0009; 0010);

decrypting the received license utilizing the session key to obtain a decrypted boundary license, wherein: the received license is an encrypted boundary license and the key within the boundary license is a boundary key (see figs. 6 and 8; 0013; 0050; 0055; 0118; 0121); and

the boundary license includes access rules for content within a rights boundary in the encrypted content that is at least one of a television program and a television channel (0105);

decrypting a content license utilizing the boundary key to obtain a content key, wherein the content license includes access rules for the encrypted content (0050; 0055; 0118; 0121); and

decrypting the encrypted content utilizing the content key, wherein the encrypted content includes at least a portion of a television broadcast (0050; 0055; 0118; 0121; 0105).

8. As per **claim 8**, Mohammed et al further discloses a method, wherein the key is

for decrypting the encrypted content (0050; 0079).

9. As per **claim 9**, Mohammed et al further discloses a method, wherein the encrypted content is streamed to the client (0070; 0072).

11. As per **claim 11 and 16**, Mohammed et al discloses a method comprising:

forming a request by a client for communication to a licensing server, wherein the request is for storing encrypted content by the client (see figs. 1, 5 and 14; 0185; 0018; 0121; 0113; 0116);

receiving a persistent license at the client in response to the request, wherein: the persistent license includes a key that is encrypted (0050; 0055; 0118; 0121);

the key, when decrypted, provides access to the encrypted content (0128);

the key is configured to be decrypted by the licensing server (0012; 0018; 0105; 0325; 0326); and

the client is not configured to decrypt the key from the persistent license (0016; 0017); and

storing the persistent license and the encrypted content by the client (see fig. 7 and 14; 0118; 0121).

12. As per **claim 12**, Mohammed et al further discloses a method, further comprising:

forming a subsequent request by the client to access the stored content, wherein the subsequent request:

is for communication to the licensing server (see fig. 5; 0017; 0096; 0146; 0155; 0156); and

includes the persistent license (see fig. 5; 0017; 0096; 0146; 0155; 0156); and

receiving a second license at the client in response to the subsequent request, wherein:

the second license includes the key (0050; 0152; 0156); and

the second license is configured to be decrypted by the client such that the client obtains access to the key (0050; 0152; 0156).

13. As per **claim 13**, Mohammed et al further discloses a method, further comprising:

forming a subsequent request by another client to access the stored content, wherein the subsequent request:

is for communication to the licensing server (figs. 5, 6 7, and 13); and

includes the persistent license (see fig. 5; 0017; 0096; 0146; 0155; 0156); and

receiving a second license at the other client in response to the subsequent request, wherein:

the second license includes the key (0017; 0096; 0146; 0155; 0156); and

the second license is configured to be decrypted by the other client such that the other client obtains access to the key (see fig. 5; 0017; 0096; 0146; 0155; 0156).

14. As per **claim 14**, Mohammed et al further discloses a method, wherein the encrypted content is streamed to the client (0070; 0072).

15. As per **claim 15**, Mohammed et al further discloses a method, wherein the license includes a certificate for verifying the licensing server by the client (0168; 0169; 0177; 0201).

17. As per **claim 17 and 22**, Mohammed et al further discloses a method comprising:

forming a first request for communication to a licensing server, wherein the first request is for storing encrypted content (see figs. 1, 5 and 14; 0185; 0018; 0121; 0113; 0116; 0155; 0156);

receiving a persistent license in response to the request, wherein the persistent license includes a boundary key (0050; 0055; 0118; 0121);

storing the persistent license and the content (see figs. 1, 5 and 14; 0185; 0130);

forming a second request to access the encrypted content, wherein the second request includes the persistent license (see figs. 1, 5 and 14; 0185; 0018; 0121; 0113; 0116; 0155; 0156);

sending the second request to the licensing server (fig. 1);

receiving a boundary license in response to the second request, wherein the boundary license includes the boundary key (0013; 0050; 0055; 0118; 0121);

decrypting the boundary license using a session key to obtain the boundary key (see figs. 6 and 8; 0013; 0050; 0055; 0118; 0121);

decrypting a content license using the boundary key to obtain a content key (see figs. 6 and 10; 0013; 0050; 0055; 0118; 0121); and

decrypting the encrypted content using the content key (figs. 5 and 10).

18. As per **claim 18**, Mohammed et al further discloses a method, wherein the forming of: the first request is performed by a first client (fig. 1); and the second request is performed by a second client (fig. 1).

19. As per **claim 19**, Mohammed et al further discloses a method, wherein the first and second requests are formed by a client (fig. 1).

20. As per **claim 20**, Mohammed et al further discloses a method, further comprising at least one of decoding the decrypted content and outputting the decoded content (see fig. 5).

21. As per **claim 21**, Mohammed et al further discloses a method, wherein: the persistent license was encrypted using an asymmetric encryption algorithm (0079); and the content, the boundary license, and the content license were encrypted using respective symmetric encryption algorithms (0050).

23. As per **claim 23**, Mohammed et al further discloses a client comprising:

a processor (fig. 12); and

memory configured to maintain:

a persistent license including a key that is encrypted (fig. 4); and

a playback application that is executable on the processor to:

form a request to access encrypted content, wherein the request:

is for communication to a licensing server (fig. 13); and

includes the persistent license (fig. 4; 0276);

receive a response to the request that includes the key (0276); and

access the encrypted content utilizing the key (fig. 3; 0016; 0276).

24. As per **claim 24**, Mohammed et al further discloses a client, wherein the key is for decrypting the encrypted content (fig. 10; 0151).

25. As per **claim 25**, Mohammed et al further discloses a client, wherein:

the memory is further configured to maintain a content license (fig. 4);

the key included in the persistent license is for decrypting the content license (fig. 1);

the content license includes a content key (fig. 1); and

the content key is for decrypting the encrypted content (figs. 1 and 10).

26. As per **claim 26**, Mohammed et al further discloses a client, wherein:

the memory is further configured to maintain a content license (fig. 4);

the key included in the persistent license is for decrypting the content license (fig. 1; 0096);

the content license includes a content key (fig. 1 and 3; 0100);

the content key is for decrypting the encrypted content (figs. 1 and 10; 0100); and

the playback application is executable to:

decrypt the content license using the key to obtain the content key (fig. 5 and 14; 0128); and

decrypt the content using the content key (figs. 1 and 10; 0100; 0128).

27. As per **claim 27**, Mohammed et al further discloses a client, wherein:

the memory is further configured to maintain a session license, a content license, and a client key (fig. 4);

the client key is for decrypting the session license (fig. 1 and 3; 0100);

the session license includes a session key for decrypting the response (0100);

the response is a boundary license (see figs. 6 and 10; 0013; 0050; 0055; 0118; 0121);

the key included in the response is a boundary key for decrypting the content license (see figs. 6 and 10; 0013; 0050; 0055; 0118; 0121);

the content license includes a content key (figs. 1 and 10; 0100; 0128); and

the content key is for decrypting the encrypted content (figs. 1 and 10; 0100; 0128).

28. As per **claim 28**, Mohammed et al further discloses a client, wherein:

the memory is further configured to maintain a session license, a content license, and a client key (see fig. 1 and 4);

the client key is for decrypting the session license (0100);

the session license includes a session key for decrypting the response (0100);

the response is a boundary license (see figs. 6 and 10; 0013; 0050; 0055; 0118; 0121);

the key included in the response is a boundary key for decrypting the content license (see figs. 6 and 10; 0013; 0050; 0055; 0118; 0121);

the content license includes a content key (fig. 1 and 3; 0100);

the content key is for decrypting the encrypted content (fig. 1 and 3; 0100); and

the playback application is executable to:

decrypt the session license using the client key to obtain the session key (0013; 0050; 0055; 0118; 0121);

decrypt the boundary license using the session key to obtain the boundary key (see figs. 6 and 10; 0013; 0050; 0055; 0118; 0121);

decrypt the content license using the boundary key to obtain the content key (see figs. 6 and 10; 0013; 0050; 0055; 0118; 0121); and

decrypt the content using the content key (figs. 1 and 10; 0100; 0128).

29. As per **claim 29**, Mohammed et al further discloses a client, wherein the playback application is further executable to:

form an initial request for:

communication to the licensing server (see figs. 6 and 13; 0017; 0155; 0156); and

storing encrypted content by the playback application (fig. 4 and 14);

receive the persistent license in response to the initial request (see figs. 5, 6 and 7; 0050; 0055; 0118; 0121); and

store the encrypted content and the persistent license (see figs. 1, 5 and 14; 0185; 0130).

30. As per **claim 30**, Mohammed et al further discloses a client, wherein the playback application is further executable to form a request to obtain the encrypted content from another client (see figs. 4, 5 and 14).

31. As per **claim 31**, Mohammed et al further discloses a client, further comprising a tuner configured to receive the encrypted content when streamed over a network (0070; 0072).

32. As per **claim 32**, Mohammed et al further discloses a client, wherein the license includes a certificate for verifying the licensing server (see fig. 10; 0168; 0169; 0177; 0201).

33. As per **claim 33**, Mohammed et al further discloses a system comprising:

a network (fig. 1 and 13);

a client including:

a persistent license having a key that is encrypted (fig. 1 and 4; 0016; 0017); and

a playback application that is executable to:

form a request to access encrypted content, wherein the request includes the persistent license (see figs. 4, 5, 6 7 and 13);

receive a response to the request that includes the key (see figs. 4, 5, 6 7 and 13; 0016); and

access the encrypted content utilizing the key (0050; 0055; 0118; 0121); and

a licensing server including a licensing module that is executable to:

receive the request including the persistent license (0276);

decrypt the persistent license to obtain the key (see figs. 6 and 10; 0013; 0050; 0055; 0118; 0121); and

form the response that includes the key for communication to the client over the network (see figs. 6, 7 and 13; 0010).

34. As per **claim 34**, Mohammed et al further discloses a system, wherein:

the client includes a content license (fig. 4);

the key included in the persistent license is for decrypting the content license (see figs. 6 and 10; 0013; 0050; 0055; 0118; 0121);

the content license includes a content key (figs. 1 and 10; 0100; 0128); and

the content key is for decrypting the encrypted content (fig. 1 and 3; 0100).

35. As per **claim 35**, Mohammed et al further discloses a system, wherein:

the client includes a content license (fig. 4, and 7);

the key included in the persistent license is for decrypting the content license (fig. 1 and 3; 0100);

the content license includes a content key (figs. 1 and 10; 0100; 0128);

the content key is for decrypting the encrypted content (fig. 1 and 3; 0100); and

the playback application is executable to:

decrypt the content license utilizing the key to obtain the content key (see figs. 6 and 10; 0013; 0050; 0055; 0118; 0121); and

decrypt the content utilizing the content key (fig. 1 and 3; 0100).

36. As per **claim 36**, Mohammed et al further discloses a system, wherein:

the client includes a session license, a content license, and a client key (see figs. 1 and 4);

the client key is for decrypting the session license (0100);

the session license includes a session key for decrypting the response (0100);

the response is a boundary license (see figs. 6 and 10; 0013; 0050; 0055; 0118; 0121);

the key included in the response is a boundary key for decrypting the content license (see figs. 6 and 10; 0013; 0050; 0055; 0118; 0121);

the content license includes a content key (figs. 1 and 10; 0100; 0128); and

the content key is for decrypting the encrypted content (fig. 1 and 3; 0100).

37. As per **claim 37**, Mohammed et al further discloses a system, wherein:

the client includes a session license, a content license, and a client key; the client key is for decrypting the session license (see figs. 1 and 4);

the session license includes a session key for decrypting the response (0100);

the response is a boundary license ();

the key included in the response is a boundary key for decrypting the content license (see figs. 6 and 10; 0013; 0050; 0055; 0118; 0121);

the content license includes a content key (figs. 1 and 10; 0100; 0128);

the content key is for decrypting the encrypted content (fig. 1 and 3; 0100); and

the playback application is executable to:

decrypt the session license utilizing the client key to obtain the boundary key (see figs. 6 and 10; 0013; 0050; 0055; 0118; 0121);

decrypt the boundary license utilizing the session key to obtain the boundary key (see figs. 6 and 10; 0013; 0050; 0055; 0118; 0121);

decrypt the content license utilizing the boundary key to obtain the content key (see figs. 6 and 10; 0013; 0050; 0055; 0118; 0121);

decrypt the content utilizing the content key (fig. 1 and 3; 0100); and

play the decrypted content (fig 5).

38. As per **claim 38**, Mohammed et al further discloses a system, wherein the key is for decrypting the encrypted content (0050; 0079).

39. As per **claim 39**, Mohammed et al further discloses a system, wherein the

persistent license is encrypted with an asymmetric encryption algorithm and the server includes a server private key for decrypting the persistent license (0050; 0079).

40. As per **claim 40**, Mohammed et al further discloses a system, wherein the playback application is further executable to: form an initial request for:

communication to the licensing server (figs. 13); and

storing encrypted content by the playback application (see figs. 1, 5 and 14; 0185);

receive the persistent license in response to the initial request (see figs. 1, 5, 7, 13 and 14; 0185); and

store the encrypted content and the persistent license (see figs. 1, 5 and 14; 0185).

41. As per **claim 41**, Mohammed et al further discloses a system, wherein the playback application is further executable to form a request to obtain the encrypted content from another client (fig. 6).

42. As per **claim 42**, Mohammed et al further discloses a system, wherein the encrypted content is streamed to the client over the network (0010; 0070; 0072).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The reference cited to Hurtado U.S. Patent 6,983,371 is a document considered relevant to the claimed invention.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Charles C. Agwumezie whose number is **(571) 272-6838**. The examiner can normally be reached on Monday – Friday 8:00 am – 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on **(571) 272 – 6712**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll free).

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington D.C. 20231

Or faxed to:

(571) 273-8300. [Official communications; including After Final communications labeled "Box AF"].

(571) 273-8300. [Informal/Draft communications, labeled "PROPOSED" or "DRAFT"].

Hand delivered responses should be brought to the United States Patent and Trademark Office Customer Service Window:

Randolph Building,

401 Dulany Street

Alexandria VA. 22314

Charlie Lion Agwumezie
Patent Examiner
Art Unit 3621
March 2, 2006

FIRMIN BACKER
PRIMARY EXAMINER